"Банктердің, Қазақстан Республикасының бейрезидент-банктері филиалдарының және банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың ақпараттық қауіпсіздігін қамтамасыз етуге қойылатын талаптарды, Ақпараттық жүйелердегі бұзушылықтар, іркілістер туралы мәліметтерді қоса алғанда, ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты беру қағидалары мен мерзімдерін бекіту туралы" Қазақстан Республикасы Ұлттық Банкі Басқармасының 2018 жылғы 27 наурыздағы № 48 қаулысына толықтыру енгізу туралы

Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігі Басқармасының 2023 жылғы 17 қазандағы № 75 қаулысы. Қазақстан Республикасының Әділет министрлігінде 2023 жылғы 20 қазанда № 33560 болып тіркелді

Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігінің Басқармасы ҚАУЛЫ ЕТЕДІ:

1. "Банктердің, Қазақстан Республикасының бейрезидент-банктері филиалдарының және банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың ақпараттық қауіпсіздігін қамтамасыз етуге қойылатын талаптарды, Ақпараттық жүйелердегі бұзушылықтар, іркілістер туралы мәліметтерді қоса алғанда, ақпараттық қауіпсіздіктің оқыс оқиғалары туралы ақпаратты беру қағидалары мен мерзімдерін бекіту туралы" Қазақстан Республикасы Ұлттық Банкі Басқармасының 2018 жылғы 27 наурыздағы № 48 қаулысына (Нормативтік құқықтық актілерді мемлекеттік тіркеу тізілімінде № 16772 болып тіркелген) мынадай толықтыру енгізілсін:

көрсетілген қаулымен бекітілген Банктердің, Қазақстан Республикасының бейрезидент-банктері филиалдарының және банк операцияларының жекелеген түрлерін жүзеге асыратын ұйымдардың ақпараттық қауіпсіздігін қамтамасыз етуге қойылатын талаптарда:

мынадай мазмұндағы 10-тараумен толықтырылсын:

"10-тарау. Банктің, ұйымның қашықтан қызмет көрсету бағдарламалық қамтылымының қауіпсіздігіне қойылатын талаптар

144. Банктің, ұйымның қашықтан қызмет көрсету бағдарламалық қамтылымына:

1) веб-қосымшалар серверлерінің бағдарламалық қамтылымы (бұдан әрі – веб-қосымша);

2) мобильді құрылғыларға арналған бағдарламалық қамтылым (бұдан әрі – мобильді қосымша);

3) бағдарламалық интерфейстердің бағдарламалық қамтылымы (бұдан әрі – серверлік ҚБҚ) кіреді.

145. Қашықтан қызмет көрсету бағдарламалық қамтылымын әзірлеу және (немесе) пысықтауды банк, ұйым бағдарламалық қамтылымды әзірлеу және (немесе) пысықтау тәртібін, әзірлеу кезеңдерін және олардың қатысушыларын регламенттейтін банктің, ұйымның ішкі құжаттарына сәйкес жүзеге асырады.

146. Банктің, ұйымның қашықтан қызмет көрсету бағдарламалық қамтылымын әзірлеу және (немесе) пысықтау тысқары ұйымға және (немесе) үшінші тұлғаға берілген жағдайда, банк, ұйым тысқары ұйымның және (немесе) үшінші тұлғаның осы тараудың және ішкі құжаттардың талаптарын орындауын қамтамасыз етеді, қашықтан қызмет көрсету бағдарламалық қамтылымның қауіпсіздігі жағдайы үшін жауап береді.

147. Банкте, ұйымда әзірленетін қашықтан қызмет көрсету бағдарламалық қамтылымның бастапқы кодтарын сақтау резервтік көшірме жасауды қамтамасыз ете отырып, банктің, ұйымның аясында орналастырылатын мамандандырылған код репозиторияларын басқару жүйесінде жүзеге асырылады.

148. Банкте, ұйымда қабылданған қашықтан қызмет көрсету бағдарламалық қамтылымды әзірлеу және (немесе) пысықтау тәсіліне қарамастан, қауіпсіздікті тестілеу міндетті кезең болып табылады, оның барысында кемінде мынадай іс-шаралар жүзеге асырылады:

1) бастапқы кодтың статикалық талдауы;

2) құрауыштардың және тысқары кітапханалардың талдауы.

149. Банктің, ұйымның қашықтан қызмет көрсету бағдарламалық қамтылымының бастапқы кодының статикалық талдауы тексерілетін бағдарламалық қамтылымда қолданылатын барлық бағдарламалау тілінің талдауын қолдайтын, бастапқы кодтың статикалық талдауының сканерін пайдаланумен жүргізіледі, оның функцияларына мынадай осалдықтарды анықтау кіреді, бірақ олармен шектелмейді:

1) зиянды кодтың кіруіне мүмкіндік беретін тетіктердің болуы;

2) осал операторларды және бағдарламалау тілдерінің функцияларын пайдалану;

3) әлсіз және осал криптографиялық алгоритмдерді қолдану;

4) белгілі бір жағдайларда қызмет көрсетуден бас тартуды немесе қосымшаның жұмысын айтарлықтай баяулатуды тудыратын кодты пайдалану;

5) қосымшаны қорғау жүйелерін айналып өту тетіктерінің болуы;

6) кодта құпияларды ашық түрде пайдалану;

7) қосымшаның қауіпсіздігін қамтамасыз ету үлгілері мен тәжірибелерін бұзу.

150. Банктің, ұйымның қашықтан қызмет көрсету бағдарламалық қамтылымының құрауыштарын және (немесе) тысқары кітапханаларын талдау құрауыштың және (немесе) тысқары кітапхананың қолданылатын нұсқасына тән белгілі осалдықтарды анықтау мақсатында, сондай-ақ құрауыштар және (немесе) тысқары кітапханалар және олардың нұсқалары арасындағы тәуелділіктерді бақылау үшін жүргізіледі.3. Осы қаулының орындалуын бақылау Қазақстан Республикасының Қаржы нарығын реттеу және дамыту агенттігі Төрағасының жетекшілік ететін орынбасарына жүктелсін.

151. Банк, ұйым атқарушы орган бекіткен ішкі құжатта айқындалған тәртіпте анықталған осалдықтарды жою жөнінде түзету шараларының іске асырылуын қамтамасыз етеді. Бұл ретте, маңызды осалдықтар қашықтан қызмет көрсету бағдарламалық қамтылымды және (немесе) оның жаңа нұсқаларын пайдалануға енгізуге дейін жойылады.

152. Банк, ұйым ақпараттық қауіпсіздік бөлімшесімен келісілгеннен кейін қашықтан қызмет көрсету бағдарламалық қамтылымын және (немесе) оның жаңа нұсқаларын пайдалануға енгізуді жүзеге асырады.

153. Банк, ұйым қашықтан қызмет көрсету бағдарламалық қамтылымының бастапқы кодтарының және соңғы 3 (үш) жыл ішінде пайдалануға енгізілген қауіпсіздікті тестілеу нәтижелерінің барлық нұсқаларын жедел режимде сақтауды және оларға қол жеткізуді қамтамасыз етеді.

154. Қашықтан қызмет көрсету бағдарламалық қамтылымының клиенттік және серверлік тараптары арасында деректер алмасу Transport Layer Security (Транспорт Лейер Секьюрити) шифрлау хаттамасының 1.2-ден төмен емес нұсқасын пайдалана отырып шифрланады.

155. Банктің, ұйымның мобильді қосымшасында клиентті бастапқы тіркеу кезінде Сәйкестендіру деректерімен алмасу орталығы (бұдан әрі – СДАО) арқылы немесе банктің, ұйымның құрылғылары арқылы алынған биометриялық деректерді пайдалана отырып, клиентті биометриялық сәйкестендіруді жүзеге асырады.

156. Мобильді қосымшаға кіру кодын (құпиясөзін) өзгерту СДАО растаған немесе банктің, ұйымның құрылғылары арқылы алынған биометриялық деректерді пайдалана отырып, клиентті биометриялық сәйкестендіруді қолданумен жүзеге асырылады.

157. Қашықтан қызмет көрсету бағдарламалық қамтылымда клиентті сәйкестендіру және бірдейлендіру банктің, ұйымның ішкі құжаттарында белгіленген қауіпсіздік рәсімдеріне сәйкес екі факторлы (үш фактордың екеуін қолдану: білім, иелену, ажырамастық) бірдейлендіру әдістерін қолдана отырып жүзеге асырылады.

158. Қашықтан қызмет көрсету бағдарламалық қамтылымды кроссдомендік бірдейлендіру тетігі ақпараттық қауіпсіздік жөніндегі бөлімшемен келісіледі.

159. Веб-қосымша:

1) веб-қосымшаның тек қана банкке, ұйымға тиесілігін сәйкестендіруді (домендік аты, логотиптері, корпоративтік түстері);

2) браузердің жадысында авторландырылған деректерді сақтауға тыйым салуды;

3) енгізілген құпияларды бүркемелеуді;

4) клиентті авторландыру парақшасында веб-қосымшаны пайдалану кезінде басшылыққа алу ұсынылатын кибергигиенаны қамтамасыз ету шаралары туралы хабардар етуді;

5) қате туралы ең аз қажетті ақпарат бере отырып, клиенттің интерфейсінде конфиденциалды деректердің көрсетілуіне жол бермей қателер мен ерекшеліктерді қауіпсіз тәсілмен өңдеуді қамтамасыз етеді.

160. Мобильді қосымша:

1) мобильді қосымшаның тек қана банкке, ұйымға тиесілігін сәйкестендіруді (қосымшалардың ресми дүкеніндегі деректер, логотиптер, корпоративтік түстер);

2) операциялық жүйенің тұтастығын бұзу және (немесе) қорғау тетіктерін айналып өту белгілерін анықтаған, қашықтан басқару процестерін анықтаған жағдайда банктің, ұйымның қашықтан қызмет көрсету бойынша функционалын бұғаттауды;

3) клиентті мобильді қосымшаның жаңартуларының бар екендігі туралы хабардар етуді;

4) маңызды осалдықтарды жою қажет болған жағдайда, мобильді қосымшаның жаңартуларын мәжбүрлеп орнату немесе оларды орнатқанға дейін мобильді қосымшаның функционалын бұғаттау мүмкіндігін;

5) конфиденциалды деректерді мобильді қосымшаның қорғалған контейнерінде немесе жүйелік есепктік деректерді сақтау орнында сақтауды;

6) конфиденциалды деректерді кэштеуді алып тастауды;

7) мобильді қосымшаның резервтік көшірмелерінен ашық түрдегі конфиденциалды деректерді алып тастауды;

8) клиентті мобильді қосымшаны пайдалану кезінде басшылыққа алу ұсынылатын кибергигиенаны қамтамасыз етудің әдістері туралы хабардар етуді;

9) клиентті оның есептік жазбасындағы авторландыру оқиғалары, құпиясөзді өзгерту және (немесе) қалпына келтіру, банк, ұйым тіркеген мобильді телефон нөмірінің өзгеруі туралы хабардар етуді;

10) ақшалай қаражатпен операцияларды жүзеге асыру барысында -клиенттің рұқсаты болған жағдайда банктің, ұйымның серверлік ҚБҚ-ға мобильді құрылғының геолокациялық деректерін беру не мұндай рұқсаттың жоқ екендігі туралы ақпарат беруді қамтамасыз етеді.

161. Банк, ұйым өз тарапынан:

1) жауапта конфиденциалды деректердің жария болуына жол бермей, проблеманы анықтау үшін ең аз қажетті ақпарат ұсына отырып, қателер мен ерекшеліктерді қауіпсіз тәсілмен өңдеуді;

2) мобильді қосымшаларды және олармен байланысты құрылғыларды сәйкестендіруді және бірдейлендіруді;

3) жалған сұрау салулармен және зиянды кодтың кірулерімен шабуылдардың алдын алу үшін деректердің жарамдылығын тексеруді қамтамасыз етеді.".

2. Ақпараттық және киберқауіпсіздік департаменті Қазақстан Республикасының заңнамасында белгіленген тәртіппен:

1) Заң департаментімен бірлесіп осы қаулыны Қазақстан Республикасының Әділет министрлігінде мемлекеттік тіркеуді;

2) осы қаулыны ресми жарияланғаннан кейін Қазақстан Республикасы Қаржы нарығын реттеу және дамыту агенттігінің ресми интернет-ресурсына орналастыруды;

3) осы қаулы мемлекеттік тіркелгеннен кейін он жұмыс күні ішінде Заң департаментіне осы тармақтың 2) тармақшасында көзделген іс-шараның орындалуы туралы мәліметтерді ұсынуды қамтамасыз етсін.

3. Осы қаулының орындалуын бақылау Қазақстан Республикасының Қаржы нарығын реттеу және дамыту агенттігі Төрағасының жетекшілік ететін орынбасарына жүктелсін.

4. Осы қаулы алғашқы ресми жарияланған күнінен кейін күнтізбелік он күн өткен соң қолданысқа енгізіледі.

Қазақстан Республикасының
Қаржы нарығын реттеу және
дамыту Агенттігінің Төрағасы *М. Абылкасымова*